DOE CIO Guidance CS-18

U.S. Department of Energy

Cyber Security Program

FOREIGN NATIONAL ACCESS TO DOE INFORMATION SYSTEMS GUIDANCE

January 2007

1. PURPOSE.

   This Department of Energy (DOE) Chief Information Officer (CIO) Guidance describes the major elements of Foreign National access to DOE/Government information and the information systems on which it resides in conjunction with DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, DOE O 142.1, *Classified Visits Involving Foreign Nationals,* and other applicable Departmental and Federal Information Systems security laws and regulations.

   A process defining Foreign National Access to DOE information systems is necessary for enforcing information access restrictions. DOE information systems include computers, networks, and associated servers, as well as data storage, switching, display, control devices, and portable/mobile devices.

   The DOE CIO will review this guidance annually and update it as necessary. DOE Senior Management and their operating units may provide feedback at any time for incorporation into the next scheduled update. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

   This Guidance enables Senior DOE Management to address the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance* and DOE Manual 205.1-4*, National Security Systems Controls Manual*, in their PCSPs. Specifically, this Guidance applies to the Access Control and Risk Assessment controls in CS-1 and User Data Protection, Security Management, and access controls in DOE M 205.1-4.

3. CANCELLATIONS.

   None.

4. APPLICABILITY.

   a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary DOE Organizations to which DOE CIO Guidance CS-18 is Applicable.*

      Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units, and for ensuring that those requirements are incorporated into contracts.

b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE guidance for activities under the NNSA Administrator's cognizance.

c. Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE systems hosting unclassified information. DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.

d. National Security Systems National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This guide is effective 30 days after issuance. However, DOE recognizes that this guide cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its issuance. If Senior DOE Management cannot address all of the criteria by that date, Senior DOE Management is to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSPs.

6. CRITERIA.

a. The Senior DOE Management PCSP must integrate the requirements of DOE O 142.1, *Classified Visits Involving Foreign Nationals*, and DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, and define policies, processes, and procedures for managing Foreign National Access to information systems to include at least the following:

(1) Roles and responsibilities of personnel involved in approving, implementing, and monitoring Foreign National Access to DOE information systems.

(2) Policy specifying the conditions for information systems, devices, media, or equipment owned by or in the possession of a Foreign National having connectivity to information systems containing DOE/Government information.

(3) Monitoring and evaluation of the effectiveness of Foreign National Access process and procedures.

(4) Specific requirements for approval, documentation, and review of Foreign National Access to information and information systems.

(5) Screening processes dependent on the security category of the information system, the information content (e.g. information types), and the level of Foreign National Access (general user, privileged user, and administrator).

(a) Foreign National Access to information systems is granted only after approval as required in DOE O 142.1 and/or DOE O 142.3.

(b) Access to Sensitive Unclassified Information (SUI) systems by Foreign Nationals must include:

i. General users must be screened to include a Human Resources Background Check and a National Agency Check.

ii. Privileged users must be screened to include a Human Resources Background Check and a National Agency Check with Inquiries.

iii. Administrators must be screened to include a Human Resources Background Check and a National Agency Check with Law and Credit.

(c) Access to National Security Systems (NSS) by Foreign Nationals must include an access approval by the system owner to the information approved through the processes described in DOE O 142.1.

(6) Prohibit Foreign National privileged users and administrators from accessing any system from other than a Senior DOE Management operating unit facility.

(7) Prohibit non-resident Foreign Nationals from Sensitive Countries from accessing information systems containing SUI or NSS from other than a Senior DOE Management operating unit facility.

(8) Prohibit Foreign National use of non-DOE equipment to access NSS.

b. Program Cyber Security Plan. Senior DOE Management PCSPs are to direct operating units to develop, document, and implement policies and procedures related to information system access by Foreign Nationals that are consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs.

(1) Access to information systems by Foreign Nationals must be approved and documented.

(a) Approval documentation must identify the applicable security plan as required by DOE O 142.1 or DOE O 142.3, the information and information system(s) to which access is granted, and the time period of the access.

(b) An official accountable for the access approval decision is to be identified in the documentation.

(c) Access is granted based on a documented assessment of risk and identification of access controls.

i. The risk assessment and approval must be referenced in the System Security Plan (SSP) and the information system access controls must be included in the SSP.

ii. The risk assessment must address the security factors (including type of area where work will be accomplished or visited, sensitivity of all information on the system, and affiliation with sensitive countries or countries identified as state sponsors of terrorism) and the results of the subject matter expert reviews for Foreign National visits and assignments as required by DOE O 142.3.

(2) Procedures for reviewing and managing Foreign National Access. The procedures must include:

(a) Documenting, monitoring, and tracking Foreign National Access to DOE information and information systems.

(b) Auditing Foreign National Access to DOE information systems consistent with the documented risk upon which the Foreign National Access approval is based.

(c) Security incident reporting concerning Foreign National Access to information systems.

(d) Training for Approval Authorities as described in DOE O 142.1 and DOE O 142.3, and Foreign National sponsor or supervisors, including contractors, regarding their Foreign National-related security obligations.

(3) Procedures to implement Department of Commerce prohibitions for US export of any encryption program or algorithm in excess of 128 bits.

(4) Prohibiting the use of encryption software of foreign governments.

7. REFERENCES.

References applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

8. DEFINITIONS.

Terms specific to this guidance are defined in Attachment 2. Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

Administrator. A user that is authorized access to control system services or files (e.g., system administration, special read, write, delete, configuration change privileges, operator, system recovery, etc.) on the system.

General user. A user that is authorized access only to general services on the system.

Human Resource (HR) Background Check. Confirmation of employment dates, job functions, and education.

National Agency Check (NAC). Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), Federal Bureau of Investigations (FBI) Name Check, and FBI National Criminal History Fingerprint Check.

National Agency Check with Inquiries (NACI). These cover specific areas of an individual's background during the past 5 years (with inquiries sent to current and former employers, schools attended, references and local law authorities). Coverage includes: Employment (5 years), Education (5 years and highest degree verified), Residence (3 years), Law Enforcement (5 years), and National Agency Check (NAC)

National Agency Check with Law and Credit (NACLC). National Agency Checks (Security/Suitability Investigations Index, Defense Clearance and Investigations Index, fingerprint classification, and a search of the Federal Bureau of Investigation's investigative index). Credit search covering all residence, employment, and education locations during the last 7 years. Law Checks covering all locations of residence, employment, and education during the last 5 years and to all locations of admitted arrest, confirms identity, credit history, legal history, reason for access.

Privileged user. A user that is authorized limited access to control system services or files (e.g., special read, write, delete, operator, system recovery, etc.) on the system.

9. CONTACT.

   Questions concerning this guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1:

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-18 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2

GLOSSARY

Approval Authority—The individual who has been assigned the responsibility and accountability to approve request for access by Foreign Nationals to one or more DOE sites, programs, information, and technologies. Officials who assign approval authority are responsible and accountable for implementing the authority assigned in a manner consistent with the requirements of DOE O 142.3 or its associated Contractor Requirements Document, and program secretarial officer guidance and management requirements.

Assignment—Foreign National access for more than 30 consecutive calendar days, but less than 2 full, consecutive years (24 consecutive months). An assignment may be extended for additional periods of up to 2 years each after completion of required reviews and approvals for each extension. Approval for assignments will be suspended any time a Foreign National assignee is unable to prove he/she is legally present in the United States.

Foreign National—A person who was born outside the jurisdiction of the United States, is a citizen of foreign government, and has not been naturalized under U.S. law.

Site—A geographical area where one or more facilities are located or a DOE-controlled land area including DOE-owned facilities (e.g., the Oak Ridge Reservation, the Nevada Test Site, the Hanford Site, Idaho National Engineering Laboratory, Rocky Flats Plant, Feed Materials Production Center).

State Sponsors of Terrorism—Countries that have been identified by the Department of State as sponsors of groups and/or activities which support terrorism or terrorist activities and are on the List of State Sponsors of Terrorism.

Subject Matter Expert—An employee who is knowledgeable about the professional standards, requirements, and practices used within the discipline he/she represents (i.e., security, export control, technology transfer, counterintelligence, or intelligence).

Visit—Access by a Foreign National for 30 calendar days or less. Approval for visits will be suspended any time a Foreign National assignee is unable to prove he/she is legally present in the United States.

Visitor—A Foreign National who has been approved to access a site, information, or technology for 30 calendar days or less.